

WHAT IS CLAIMED IS:

1. A method for handoff in a wireless communication network, comprising:
generating a handoff encryption key;
handing off a wireless terminal from a first access point to a second access point;
and
communicating data packets encrypted with the handoff encryption key between
the second access point and the wireless terminal for immediate secured data transmission before
authentication of the wireless terminal is completed.
2. The method according to claim 1, wherein the handoff encryption key is a handoff
WEP (Wired Equivalent Privacy) key.
3. The method according to claim 1, wherein the handoff encryption key is
generated by an authentication server.
4. The method according to claim 3, wherein the authentication server is an AAAH
(Authentication, Authorization, and Accounting Home) server.
5. The method according to claim 3, wherein the authentication server is an AAAF
(Authentication, Authorization, and Accounting Foreign) server.
6. The method according to claim 3, wherein the handoff encryption key is
generated according to IEEE 802.11.
7. The method according to claim 3, further comprising transmitting the handoff
encryption key to the first and second access points.
8. The method according to claim 7, further comprising, at the first access point
transmitting the handoff encryption key to the wireless terminal.

9. The method according to claim 8, further comprising, at the second access point decrypting data from the wireless terminal with the handoff encryption key.

10. The method according to claim 3, further comprising communicating handoff authentication messages between the wireless terminal and the second access points.

11. The method according to claim 10, further comprising encrypting the handoff authentication messages with the handoff encryption key.

12. The method according to claim 1, wherein the handoff encryption key is generated by the first and second access points as a function of common handoff encryption key generation information from an authentication server.

13. The method according to claim 1, further comprising, at the second access point, determining whether a packet received is encrypted by the handoff encryption key.

14. The method according to claim 13, further comprising, at the second access point, decrypting a packet encrypted by the handoff encryption key.

15. The method according to claim 1, wherein the first access point and the second access point receive a common handoff authentication key generation process from an authentication server.

16. The method according to claim 15, further comprising:

- providing a secret parameter to a handoff encryption key generator associated with the first access point;
- providing an open parameter to the handoff encryption key generator associated with the first access point; and

generating the handoff encryption key as a function of the secret parameter and the open parameter.

17. The method according to claim 16, wherein the secret parameter comprises information about the authentication server.

18. The method according to claim 17, wherein the secret parameter comprises ID information of the authentication server and at least one common parameter of the authentication server.

19. The method according to claim 16, wherein the open parameter comprises information about the first access point.

20. The method according to claim 16, wherein the open parameter comprises information about the wireless terminal.

21. The method according to claim 16, wherein the open parameter comprises the address of the first access point and the address of the wireless terminal.

22. The method according to claim 16, further comprising transmitting the handoff encryption key from the first access point to the wireless terminal.

23. The method according to claim 16, further comprising, at the wireless terminal, transmitting to the second access point data encrypted by the handoff encryption key.

24. The method according to claim 16, further comprising, at the second access point, obtaining the address of the first access point.

25. The method according to claim 16, further comprising, at the second access point, obtaining the address of the wireless terminal.

26. The method according to claim 16, further comprising, at the second access point, deriving the handoff encryption key according to the key generation process.

27. The method according to claim 16, further comprising, at the second access point, decrypting data from the wireless terminal with the handoff encryption key.

28. A wireless communication network comprising:

an authentication server operable to generate and transmit a handoff encryption key;

a first access point, receiving the handoff encryption key; and

a second access point, receiving the handoff encryption key from the authentication server and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed.

29. The wireless communication network according to claim 28, wherein the handoff encryption key is a handoff WEP (Wired Equivalent Privacy) key.

30. The wireless communication network according to claim 28, wherein the authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server.

31. The wireless communication network according to claim 28, wherein the authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server.

32. The wireless communication network according to claim 28, wherein the handoff encryption key is generated according to IEEE 802.11.

33. The wireless communication network according to claim 28, wherein the second access point communicates handoff authentication messages with the wireless terminal.

34. A wireless communication network comprising:

an authentication server operable to generate and transmit handoff encryption key generation information;

a first access point, generating a first handoff encryption key as a first function of the handoff encryption key generation information; and

a second access point, generating a second handoff encryption key as a second function of the handoff encryption key generation information and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed.

35. The wireless communication network according to claim 34, wherein the handoff encryption key is a handoff WEP (Wired Equivalent Privacy) key.

36. The wireless communication network according to claim 34, wherein the authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server.

37. The wireless communication network according to claim 36, wherein the AAAH server communicates with the first and second access points via an AAAF (Authentication, Authorization, and Accounting Foreign) server.

38. The wireless communication network according to claim 37, wherein the AAAF server communicates with the first and second access points via a router.

39. The wireless communication network according to claim 34, wherein the authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server.

40. The wireless communication network according to claim 34, wherein the second access point communicates handoff authentication messages with the wireless terminal.

41. A wireless communication network comprising:

an authentication server operable to generate and transmit a handoff encryption key generation secret parameter;

a handoff encryption key generator, generating a handoff encryption key as a function of the handoff encryption key generation secret parameter and an open parameter;

a first access point, transmitting the handoff encryption key; and

a second access point, deriving the handoff encryption key and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed.

42. The wireless communication network according to claim 41, wherein the secret parameter comprises information about the authentication server.

43. The wireless communication network according to claim 42, wherein the secret parameter comprises ID information of the authentication server and common parameter of the authentication server.

44. The wireless communication network according to claim 41, wherein the open parameter comprises information about the first access point.

45. The wireless communication network according to claim 41, wherein the open parameter comprises information about the wireless terminal.

46. The wireless communication network according to claim 41, wherein the open parameter for the first access point comprises the address of the first access point and the address of the wireless terminal.

47. The wireless communication network according to claim 41, wherein the second access point obtains the address of the first access point.

48. The wireless communication network according to claim 41, wherein the second access point obtains the address of the wireless terminal.

49. A wireless communication network comprising:

a first authentication server operable to generate and transmit a first handoff encryption key;

a second authentication server operable to generate and transmit a second handoff encryption key;

a first access point, receiving the first handoff encryption key; and

a second access point, receiving both the first handoff encryption key and the second handoff encryption key, and decrypting encrypted data from a wireless terminal before authentication of the wireless terminal is completed.

50. The wireless communication network according to claim 49, wherein the first authentication server is an AAAF (Authentication, Authorization, and Accounting Foreign) server.

51. The wireless communication network according to claim 49, wherein the first authentication server is an AAAH (Authentication, Authorization, and Accounting Home) server.

52. The wireless communication network according to claim 51, wherein the first authentication server communicates with the first and second access points via an AAAF (Authentication, Authorization, and Accounting Foreign) server.

53. A wireless access point comprising a memory which stores:

instructions to receive a handoff encryption key generation secret parameter from an authentication server;

instructions to receive a first packet from a wireless terminal, wherein the first packet includes an address of the wireless terminal;

instructions to generate a handoff encryption key as a function of the handoff encryption key generation secret parameter and the address of the wireless terminal; and

instructions to transmit the handoff encryption key to a wireless terminal.

54. The wireless access point according to claim 53, where the memory further stores:

instructions to receive a second packet from the wireless terminal;

instructions to decrypt data in the second packet with the handoff encryption key;

and

instructions to transmit the decrypted data.

55. A wireless access point comprising a memory which stores:

instructions to receive a handoff encryption key from an authentication server;

instructions to transmit the handoff encryption key to a first wireless terminal;

instructions to receive data encrypted with the handoff encryption key from a second wireless terminal;

instructions to decrypt the data with the handoff encryption key before authentication of the second wireless terminal is completed; and

instructions to transmit the decrypted data.

56. A wireless access point comprising a memory which stores:

instructions to receive a handoff encryption key generation information from an authentication server;

instructions to receive data from a wireless terminal;

instructions to generate a handoff encryption key based on the handoff encryption key generation information and the data;

instructions to decrypt the data with the handoff encryption key before authentication of the wireless terminal is completed; and

instructions to transmit the decrypted data.

57. A handoff encryption key generator in a wireless communication network, comprising:

an input to receive a handoff encryption key generation secret parameter;

an input to receive an open parameter; and

a generator for generating a handoff encryption key as a function of the handoff encryption key generation secret parameter and the open parameter.

58. The handoff encryption key generator according to claim 57, wherein the secret parameter comprises information about an authentication server.

59. The handoff encryption key generator according to claim 57, wherein the secret parameter comprises ID information of the authentication server and at least one common parameter of the authentication server.

60. The handoff encryption key generator according to claim 57, wherein the open parameter comprises information about an access point.

61. The handoff encryption key generator according to claim 57, wherein the open parameter comprises information about a wireless terminal.

62. The handoff encryption key generator according to claim 57, wherein the open parameter comprises the address of an access point and the address of a wireless terminal.

63. A wireless terminal in a wireless communication network, comprising a memory which stores:

instructions to receive a handoff encryption key from a first access point;

instructions to encrypt output data with the handoff encryption key; and

instructions to send the encrypted data to a second access point before authentication of the wireless terminal is completed.